Infosec incidents

- practical incident management
- computer forensics

Peeter Tatter

Infosec incidents

- Situation, when SomeThing:
  - .. does not work quite well
  - .. is missing
  - .. too much of it (lines in logfile)
  - ..

First steps after identifying incident

- First step – what it is about

Organizational steps

  - Who is qualified to decide, what to do?
  - Is there The Action Plan?
  - Who is involved and who should be involved?

- Can the incident end with police investigation?

Analysis of the initial information

- Important first questions:
  - When, who, what noticed?
  - What has been done already and what has happened after that?
  - How to obtain more detailed information?
  - What to do next?
  - How to manage information?

Restoring services vs preserving evidence

- How to restore services ASAP?
  - Use backup system, leave compromised system for analysis
  - Restore system to new media, leave media of the compromised system for later analysis
  - .. or .. let's try to restore services somehow and'll worry other things later (cost efficient, we „had“ a backup)

Collecting information, sources

- computers
- logs
  - servers
  - firewalls
  - Access and security systems
- Security camera recordings
- People
- Backup copies

Storing and transporting collected data

- With computers:
  - Store the PC/server
  - Store media
  - Make copy of the media
  - Copy only files
- logfiles
  - Do not filter – or – preserve as much as possible
  - cryptohash everything

Analysing data inside the computer

IMPORTANT! Avoid altering data.

Traditional approach:

- Do not power on
- Do not use running computer, remove power (battery from laptop)
- What was connected and where ... ?
- Disconnect peripherials, take computer and go ...

Basic rules

Avoid using the original system

- Never run the system from original media
- Remove and duplicate media
- Sometimes you may run computer from live-cd

Rule – store original data and work on the copy

Copying the data for analysis

preferred:

- *cloning*
- *disk imaging*

- *volume imaging*
- *logical imaging*
- *copying*

Copying ....

Checking the authenticity

- Checksum clone, image (MD5/SHA1)
- Checksum smaller data blocks (CRC)
- Checksum files

Copying ...

Formats

- dd (*raw image*)
  - Most universal
  - No automatic checksumming
- E0x
  - *de facto* (EnCase) /some years ago .../
  - Automatic checksumming (MD5, CRC)
  - Includes image metadata describing media
  - Closed data format :-(

Copying …

Selecting OS:

- Linux
- Live CD-d (Helix)
- Something special

Copying ...

Forensic disc duplicators:

- Portable independent device
- Cloning and duplicating
- Speed <4GB/min
- Checksumming during cloning
- Automatic logging

Commonly used devices:

- Logicube MD5/Talon/Quest
- Tableau TD1
- ImageMASSter Solo

After copying ...

What's next?

- Checksum both – original and clone - NOW!
- Write down date/time of the computer
- Make backup of the cloned/copied data

Now, let's analyze ...

Analyzing

- Interpreting filesystems
  - FAT12, FAT16, FAT32
  - NTFS
  - EXT2/EXT3, Reiser
  - HFS/HFS+
  - FFS/UFS/UFS2
  - ISO9660/Joliet/UDF

Analyzing

- Restoring erased files:
  - Data is erased when it is overwritten
  - Interpreting filedescriptors of deleted files on filesystem level
  - ...
  - No miracles if information has been overwritten
  - SSD “problems” can help, mostly fixed

Analyzing

- Space unused by the filesystem
  - Unused clusters
  - Physical and logical size of the file (*file slack*)
  - Unpartitioned space

This space can be filled with data, how to find it?

Analyzing

Keyword search

- Realtime search
- Indexed search
- regexp-search

- different encondings (ä, ц, や)

Analyzing

- Preview of file contents
- Picture gallery
- Using file type signature database
- Checksum comparison
- (semi)automatic documenting, summaries ...

Tools

Historical:

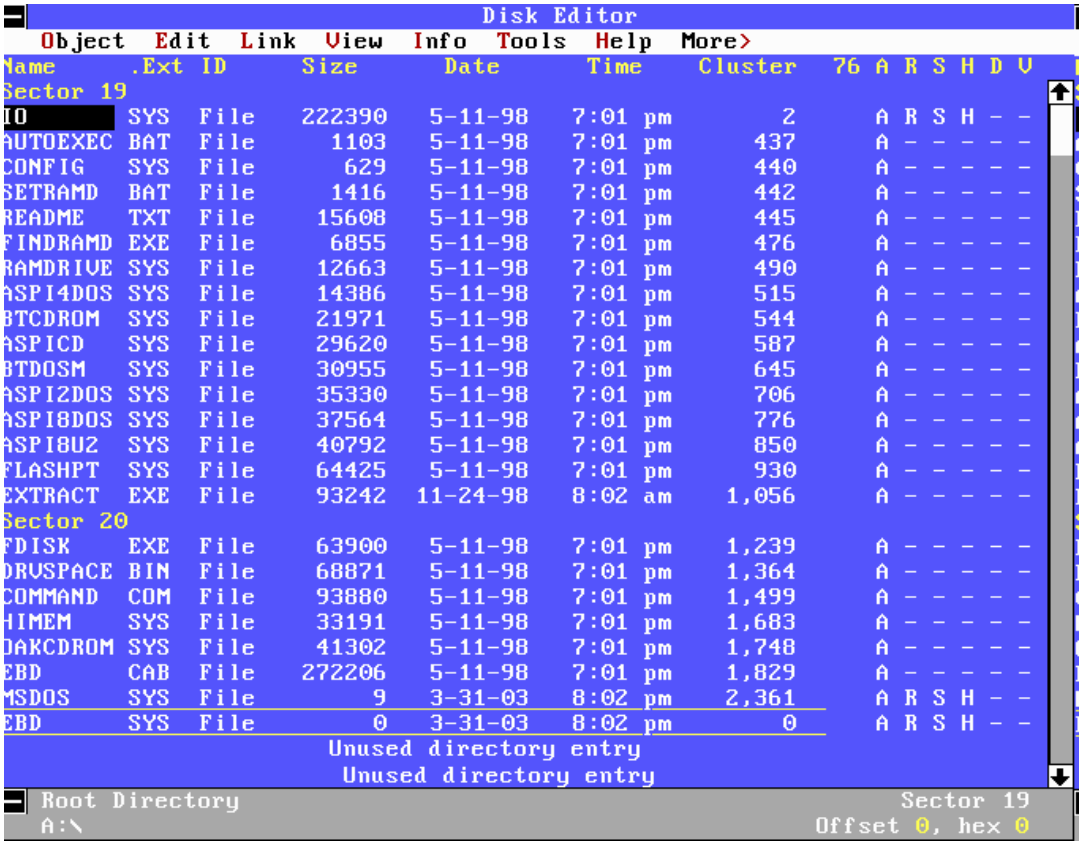
- Norton Disk Edit (diskedit.exe)
- TCT - The Coroners Toolkit

Current:

- TSK (The Sleuth Kit)
  - Autopsy
  - PTK
- EnCase
- FTK (Forensic Toolkit)
- X-Ways Forensics (WinHex)

Tools - Norton Disk Edit

- One of the first
- Is not specialised
- Can interpret only FAT-filesystem
- Mostly used as a learning tool
- Lot's of forks and developments based on it



Tools - TCT

The Coroners Toolkit

- Presented 1991,
  D. Farmer ja W. Vienema
- Minly for analyzing
  Unix'es
- Collection of CLI tools,
  Perl ja C
- Free
  (IBM Public Licence)

René Magritte "La trahison des images"

http://www.porcupine.org/forensics/tct.html

Tools - TSK

The Sleuth Kit

- Collection of CLI tools
- Improved TCT
- Supports: Linux, OS X, FreeBSD, OpenBSD, and Solaris
- Recognizes FAT, NTFS, UFS, EXT2FS, and EXT3FS
- Free (CPL, IBM Public License)

http://www.sleuthkit.org/sleuthkit/

Tools – Autopsy ja PTK

GUI for TSK

- Autopsy – created by TSK team
- PTK – alternative by DFLabs

http://www.sleuthkit.org/autopsy/
http://ptk.dflabs.com/

Tools - EnCase

- MS Windows based tool
- Very common, *de facto* standard
- Intuitive and user friendly GUI
- Modular design
- Good end user support and active community
- Closed source commercial software, quite expensive

Tools - FTK

- MS Windows based
- Second most popular
- User friendly, less technical than EnCase, less options
- Powerful indexing search engine
- Some filesystems are supported
- Closed source commercial software

Tools – comparison

- CLI tools may be problematic when analyzing big case. Requires self dicipline.
- Using GUI tools may end with random „surfing“
- Best tools are really, really expensive
- There is no universal tool!

„*Traditional forensics*“ vs „*live forensics*”

Traditional forensics

- Avoid tampering original data

Live forensics

- Avoid tampering original data and store data in the memory

Analyzing powered on computer

Additional data from powered-on computer:

- Active processes and data about them
- Information about network connections
- Mounted external disks, crypto containers
- Other data in the RAM

How to store all this and avoid tampering data on the media?

Analyzing powered on computer

Manually

- Applications, processes, network connections ...
- Mounted media, copy of mounted media ...
- …
- Power off, and back to step one (copy media ...)

Avoid, if possible ...

Analyzing working computer

Tools for dumping memory:

- psinfo/pslist/psfile/psloggedon (SysInternals)
- PMDump/MemImager (Arne Vidstrom)
- mdd (SourceForge)
- winen (EnCase paketis)

Analyzing working computer

Tools for automated analysis:

- WFT (Windows Forensic Toolchest)
- COFEE (Computer Online Forensic Evidence Extractor) /by Microsoft/

Finally

- Leave it to professionals
- Be prepared for the worst (as a potential victim)
- If you are targeted, try to preserve as much evidence as possible
- Time factor …